Physica A 403 (2014) 45–53

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

Comparisons of complex network based models and direct current power flow model to analyze power grid vulnerability under intentional attacks

Min Ouyang [*], Lijing Zhao, Zhezhe Pan, Liu Hong

School of Automation, Huazhong University of Science and Technology, 1037 Luoyu Road, Wuhan, 430074, China

HIGHLIGHTS

- We test effectiveness of complex-network theory to assess power grid vulnerability.
- We consider purely topological model (PTM) and betweenness based model (BBM).
- BBM and PTM both produce real topological vulnerability at small attack intensity.
- PTM can better estimate real flow-based vulnerability under attacks than BBM.

ARTICLE INFO

Article history:
Received 3 August 2013
Received in revised form 29 January 2014
Available online 15 February 2014

Keywords:
Power grid
Complex network models
Direct current flow
Vulnerability
Intentional attack

ABSTRACT

Many scholars have applied complex network based models to investigate power grid vulnerability, but how effective are these models to capture the real performance is an interesting topic. This paper selects two typical complex network based models, including a purely topological model (PTM) and a betweenness based model (BBM), as well as a direct current power flow model (DCPFM), to simulate the topology-based and flow-based vulnerability of power grid under degree, betweenness, maximum traffic and importance based intentional attacks. The relationships of vulnerability results from different models are analyzed and discussed for model comparisons. Taking IEEE 300 power grid with line capacity set proportional to tolerant parameter *tp* as example, the results show that there exists a critical node attack intensity $AI = 0.147$, above which the three models produce almost identical topology-based vulnerability results under each attack strategy at any $tp \geqslant 1$, while producing identical flow-based vulnerability results from PTM and DCPFM occurs at $AI > 0.147$, and $AI > 0.73$ for BBM and DCPFM, which indicates that the PTM can better approach the DCPFM for flow-based vulnerability analysis under intentional attacks. Similar results are also found for intentional edge attacks and other power grids.

1. Introduction

Infrastructure systems, including transportation, water, gas and oil, electric systems and so on, play a critical role in social activities. Among them, electric systems are particularly important because many other systems rely on the electricity for operation [1]. However, their importance may be utilized by terrorists or enemies to attack a region or country. Hence, many scholars have proposed different models and studied power grid vulnerability to identify critical components for their protection. Here, for the term "vulnerability", scholars in the engineering field have proposed different definitions [2–6].

[*] Corresponding author. Tel.: +86 027 87559490.
E-mail addresses: mouyang618@gmail.com, min.ouyang@hust.edu.cn (M. Ouyang).

http://dx.doi.org/10.1016/j.physa.2014.01.070
0378-4371/© 2014 Elsevier B.V. All rights reserved.

Considering these available literature, this paper quantifies the vulnerability as the performance drop of a power grid under a disruptive event. In the literature, power grid vulnerability models can be simply grouped into two types.

The first type is the complex-network based vulnerability models, which represent power grids by networks, with the generators and substations represented as nodes and the electrical wires as edges, and then study network response of the power grids under disruptive events. Some studies do not consider the particle transportation and redistribution on the power grids and measure the system performance drop only according to the topological change, where the performance is usually measured by the size of largest connected sub-grid [7], the connectivity level or loss [8], the fraction of affected customers [9] and so on. These studies include the vulnerability analysis of the North American power grid [7] and European power grid [10] under intentional attacks, the vulnerability assessment of power grids of some countries in European Union (Italy, French, Spain) [11] as well as the Nordic and Western USA [12] under multiple component failures. However, these studies cannot capture the dynamics of particles and the overload-induced cascading failures over power grids. Hence, some other studies assume artificial particle flow over power grids along some routine, such as the shortest paths, and define the node and link load levels according to network topological properties, such as betweenness and degree. A disruptive event can cause some component failures and alter a power grid topology, which further changes all components' loads and causes some components overloaded and failed until all remaining components' load less than their own capacities. These studies include the vulnerability analysis of Western US power transmission grid [13], North American power grid [14] and Italian power grid [15] under both random and intentional failures, IEEE 118 power grid [16] and several power grids in Texas, USA [17,18] under natural hazards and so on.

The second type is real power flow models, which use the power balance equations and electrical engineering constraints to describe the quantities and distribution of particles over power grids. To capture the power grid behavior, the alternative current (AC) power flow model is the most accurate one. This model analytically determines the real and reactive flows over all the lines by using the real and reactive balance equations to solve the voltage magnitude and phase angles at each substation, and is used for vulnerability study of South-Western part of the transmission grids of England and Wales under weather hazards [19]. However, this model is very complicated due to its non-linear feature, hence some direct current (DC) power flow models (DCPFM) have been proposed in the literature. This type of models uses a linear equation to reflect the relationship between power flow vector through the lines and the power injection vector at the nodes, and has been adapted to many detailed models to capture different aspects of power grids, such as the DC based OPA model which accounts for the system long-term evolution [20–22], the hidden failure based DC power flow model which captures the malfunction of protective relays [23], and the stochastic DC power flow model which captures uncertainties during the initial failure stage, cascading failure stage and the restoration stage [24].

As the complex network based models overlook the electric engineering properties, the vulnerability analysis results from them could be far from the results from the real power flow models. Hence, Ouyang [25] analyzed and compared the vulnerability results from the complex network based models and DC power flow based model under random failures, and found that when the power line capacity is large enough or the fraction of failed components exceeds a certain value, the complex network based models can produce identical results with those from the DC power flow model. Under the intentional attacks, i.e. the worst failure scenarios, whether the above critical power lines capacity and the critical fraction of failed components are still the same with those under random failures and which one of the complex network models can better simulate DCPFM will be further discussed in this paper.

The rest of this paper is organized as follows: Section 2 introduces the vulnerability models and the intentional attack strategies. Section 3 takes the IEEE 300 power grid as an example to compare the vulnerability results from different models under intentional node attacks and analyze which one of the complex network models can better describe the behavior of the DC power flow model. Section 4 further discusses the findings under other power grids and other attacks. Section 5 provides conclusions and future research.

2. Power grid vulnerability models and attack strategies

As a subsequent research of the work in Ref. [25], which compares the vulnerability results from purely topology model (PTM), betweenness based model (BBM) and direct current (DC) power flow model (DCPFM) to discuss how effective the complex network based models can analyze power grid vulnerability under multiple random component failures, this paper further compares the vulnerability results from these three models under intentional attacks. This section will first provide two vulnerability metrics and a brief introduction of the three models (readers can refer to Ref. [25] for more details) and then introduce several intentional attack strategies for model comparisons.

The first vulnerability metric is a topology-based metric and called as the connectivity loss, which measures the drop of connectivity level between generators and load substations and is defined by the following equation for an initially connected grid:

$$V_{\mathrm{CL}} = 1 - \frac{1}{n_D} \sum_{i=1}^{n_D} \frac{n^i_{G,\mathrm{damg}}}{n_{G,\mathrm{norm}}} \tag{2.1}$$

where n_D is the number of load substations, $n_{G,\mathrm{norm}}$ is the number of generators in the normal power grid, and $n^i_{G,\mathrm{damg}}$ is the number of generators connected to the ith load substation in the damaged power grid.